Roope Hokkanen

Information security in an organizational environment

Bachelor’s thesis

Information technology

2020

South-Eastern Finland
University of Applied Sciences

Author (authors)	Degree title	Time
Roope Hokkanen	Bachelor of Engineering	May 2020

Thesis title

33 pages

Information security in an organizational environment

Commissioned by

Supervisor

Matti Juutilainen

Abstract

In this thesis the approach was learning about information security in an organizational environment through research, statistics and examination. Studying the security methods organizations currently take to combat the issue of cybersecurity. Using data gathered from real life events, surveys and research papers to analyze where information security lacks most in organizations. Another focus point of this thesis was studying how organizations currently fight to prevent breaches from happening and making observations on where security procedures need to focus more going forward. To understand how and why the breaches happen, understanding of the methods and strategies hackers use is key.

Studying 3 major incidents from past years on how the hackers were able to find vulnerabilities from a major organization to leverage unauthorized access to their systems. All 3 incidents caused massive financial damages for the organization. The 3 cases of data breaches studied in this thesis were among the biggest we have had in the past 15 years. All against well established organizations expected to be able to handle information securely.

The practical part of this thesis was to set up a real penetration testing environment used by professionals alike around the world. Using Kali linux and metasploitable 2 to create a safe virtual environment for research, practice and training purposes. With the environment 2 example hacking tools are showcased as a proof-of-concept to the theory part. A packet sniffing hack shows the vulnerability of an unsafe network and how easy it could possibly be to capture sensitive data over an untrusted connection. A web server analyzer is a tool that searches vulnerabilities from the protocols and technologies used in a web server. A tool like this was used find the vulnerability in one of the study cases.

Observations from the thesis conclude that the cybersecurity threats are an ever-growing issue and the development in steps to prevent attacks are not keeping up with the demand. Human error is the weakest link of most organizations that causes the most vulnerabilities. Organizations need to focus on all areas, but it all starts from people.

Keywords

Information security, cybersecurity, hacking, penetration testing

CONTENTS

1 INTRODUCTION

The increasing use of internet applications to handle sensitive personal information is apparent in everyone's everyday life. Undoubtedly, the services we have access to on our devices make our lives easier. The worrying part of this is that there is seemingly endless amounts of applications and services that require our personal information to use. The more widely we spread our information, more likely we are to be a victim of identity theft or fraud. Most people take their privacy for granted and trust the companies to handle the information securely. Although security measures between companies vary, information is never completely safe. Time after time, big and seemingly impenetrable systems get breached and massive amounts of sensitive data get leaked. If this can happen to the companies of that size and structure, how safe are the smaller ones?

The purpose of this study is to learn about information security in an organizational setting, analyse past incidents and examine the consequences of data breaches. With the information available on the large data breaches that have occurred in the past 15 year, the aftermath of each case is different. A recurring theme of each case is an individual with much less resources was able find a vulnerability and use that to gain unauthorized access to sensitive information. Companies keep evolving their security measures constantly, just to stay ahead of hackers, who are also constantly getting better. On the other end of the spectrum, there is every individual's own personal information security measures, starting from passwords. Understanding what happens when we input credentials to our favourite application on mobile device and where the possible vulnerabilities lie.

The practical part of this thesis includes setting up a penetration testing environment and running an example hack. All actions will be performed on virtual machines running on a private secluded network. I will also examine methods in which the vulnerabilities of web servers can be found via web server scanners.

The goal is to get a clear picture of what vulnerabilities modern society's everyday lifestyle puts on us and organizations, where we rely on devices for everything we do. Vulnerabilities concern everyone, from large companies to average consumers.

2 INFORMATION SECURITY

Information in this context means any data or content with value to the given person or organization. Information security stands for preservation of integrity and secrecy during information transmission or storage. Breaches of the security occur when unauthorized person or party accesses the information. These can be result of actions by hackers, criminals, competitors or employees.

2.1 Confidentiality, integrity and availability

Information security can be represented by these three basic principles, Confidentiality, integrity and availability also known as CIA Triad.
Following the description for each principle from a publication by Keung Y.H (2014), we can understand each principle as follows.

Confidentiality stands for keeping data availability restricted to only the appropriate group. Access to this data is controlled and data has not been compromised by unauthorized parties. A failure in confidentiality comes when information has been accessible to someone who wasn't supposed to access it. This can be a result of intentional or accidental behavior. Failure of a confidentiality is also known as *breach.* Almost all major security incidents that we hear about in the media include massive breaches of confidentiality.

Integrity of data means authenticity of information, ensuring that it has not been altered, tampered or destroyed. Integrity also ensures the genuineness of the source. An example of a failure in integrity could be, if an attacker was able to change the information on a website as he pleases.

Availability corresponds to data being available when it is required as well as the workability of the system. To ensure accessibility at all times, precautions against power cuts, natural disasters and hardware failures are put into place. Attacks against availability may include denial of service (DoS) types of attacks, where the goal is to bring down availability of normal users.

2.2 Security measures

To support the basic principles of information security, security measures are used to account for possible attacks, user errors, accidents and failures. Different features, mechanisms and protocols are used in each step of accessing sensitive information. The following grouping is based on the article by Victoria (2019).

- Physical controls of the environment are used to limit access and outside contact to the information infrastructure. Examples could be doors, locks, walls, shields.
- Logical controls are used to manage who can access the electronic information. To achieve this, technologies like encryption, digital signatures and authentication are used. But the most utilized logical security measure we use is passwords.

Organizations are faced with potential losses and other mischievous impact on systems, resulting in the need to examine all the areas to improve security if they want to increase their odds of having a secure environment. Based on Cisco annual Cybersecurity report (2018) Cisco’s 2017 assessments indicated the key defensive capabilities: people, policies and technology that are introduced in Figure 1.

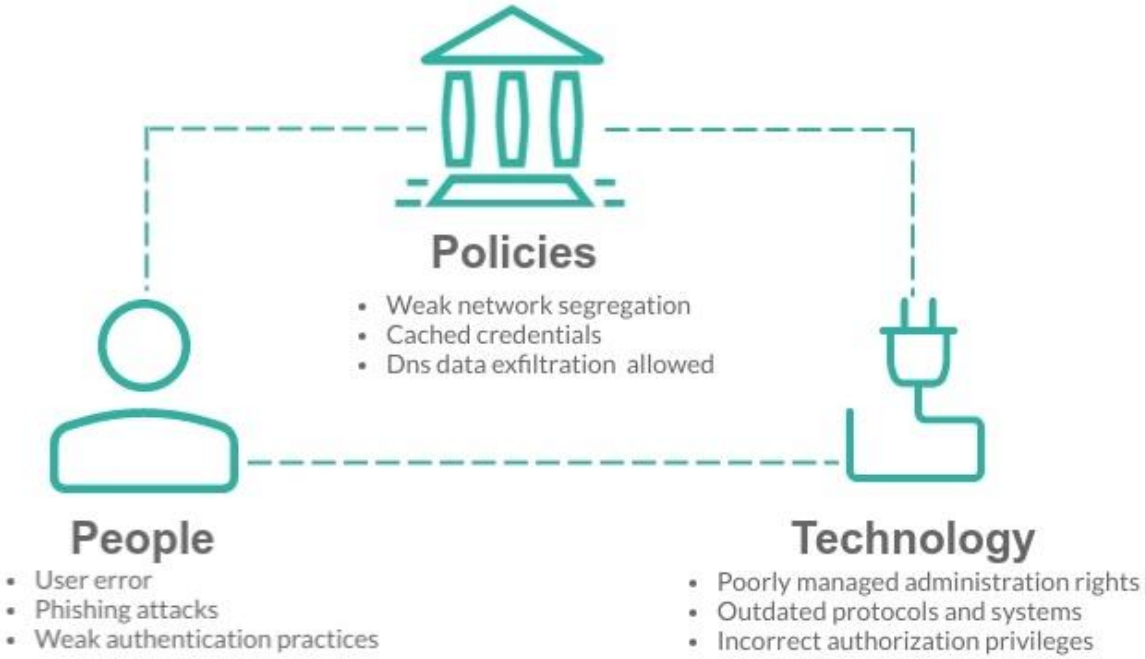

Figure 1. Cisco annual Cybersecurity report key defensive capabilities

Organizations can't rely on the technology alone to remediate security vulnerabilities. As the Cisco attack simulations show, around 26 percent of the issues identified would be solved by technology alone, which would leave 74 percent of the issues unresolved (Figure 2).

Figure 2. Only 26 percent of security issues solved by technology alone

Encryption

Following description of what is encryption, found on Cloudfare (2019). Data encryption is one of the most important security methods used in network communications. It allows for safe information transfer over network maximizing the confidentiality and integrity of the data. Information is encoded into what is called ciphertext, which is unreadable form of the information. Only the parties with the right encryption key are then able to decrypt it, and access it.

Access control

This section bases on the RSI Security blog (2019) on the purpose of information security controls. Access control has an essential role in information security. For example, in a company, most employees will not need to access all the company information and resources. Instead they can work with the specific information that concerns them. Primarily the access control consists of the following three restriction methods.

1. **Identification** is the first step to verify that the person says who they say. Most often, universal naming system is used, which can be implemented based on a username or account number. Usernames should follow a couple of practices for effective and safe identification. Each name should be unique to ensure culpability. Users should keep their usernames undisclosed. Usernames should not refer to anything else than the person itself, for example, persons title in the organization.
2. **Authentication** is used to prove the identity of the user. The three most used authentication methods all provide different levels of security. Passwords and pins are the most commonly used method of authentication, the cheapest to implement, but as a result also the least secure. Access cards and keys provide a digital signature or two-step factor authentication to increase security. Out of the three, biometrics is the most costly and secure authentication method, using genetic characteristics and attributes to confirm person identity. The most familiar example of a biometric authentication would be a fingerprint scan.

3. **Authorization** controls what the identified and authenticated person can do, in terms of changing, editing and removing to given data. Authorization also controls the ability of accessing certain areas and resources.

When Implementing a well-working access control system, there are things that need to be taken into consideration when choosing the most suitable methods. The user types need the be identified. Internal users are the employees and other personnel who require continuing access. Whereas the customers would be identified as external users. Sometimes, access needs to be granted for a temporary time period. For example, maintenance crew might require some level of access. These limited time users can be granted different levels of access depending on the nature of their objective. The system implemented for access control management needs to be dynamic to account for changing user privileges. This minimizes excessive privileges being left out on users that no longer require them. Just as the users, the same principle can apply to the devices used to access. Controlling the devices that can connect any secure network is a major factor from a security standpoint. Data classification is used to control resources by giving them more or less restrictions. A simplified example of data classification could be to categorize resources into confidential, private, public or internal. This allows for control over who can access what resources.

2.2.1 End-user cyber security awareness

Article by Fahey (2019) stated the importance of end-user security awareness. End-users are usually the weakest link of any secure environment, which is why threat origin seeks options to abuse this vulnerability. With the modern-day devices becoming more transportable and multifunctional, the risks associated with them are also increasing. For example, bringing an infected device into a secure network could cause the infection to spread throughout the network and cause further harm. Many of the users that are connected to secure private networks at some point during the day, don’t have awareness of basic security practices. The problem is that most users don’t understand the importance of privacy, until they have lost it.

The article on Infosec (2015) had 12 information security experts weigh in on the end-user security awareness. What could be learnt from the article where the conjunctive theme was end user training? Based on the article, some of the most effective personal security practices that protect users and networks they are connected to include having a strong authentication and using common sense. Keeping your devices and software up to date on the updates also significantly improves the chances against falling as a victim to cybercriminals.

Now, having a unique and strong password on each of the services we use can prove to be very laborious. The solution that is recommended to users by cybersecurity experts around the world is a password manager. Password managers provide secure authentication by means of unique and complex passwords to all our required services and devices, in a very user-friendly manner. Different password manager providers offer different level of authentication methods and other features. Based on the explanation found in Pixelprivacy (2020), understanding the working principle of password managers is quite simple (Figure 3). Password managers allow storing login credentials securely in a central location and automatically retrieving them when trying to log in to a service or device. All the data stored in a password manager is secured by a layer of AES-256 encryption. Most of the password managers are cloud based services that require internet connection on the device.

Figure 3. Password manager

Onelogin (2019) explains what multi-factor authentication is and how it works. Another very effective tool for authentication is multi-factor authentication which requires two or more authentication methods to be applied in order to grant access (Figure 4). The use of multi-factor authentication is gaining traction, as it is constantly becoming more and more available.

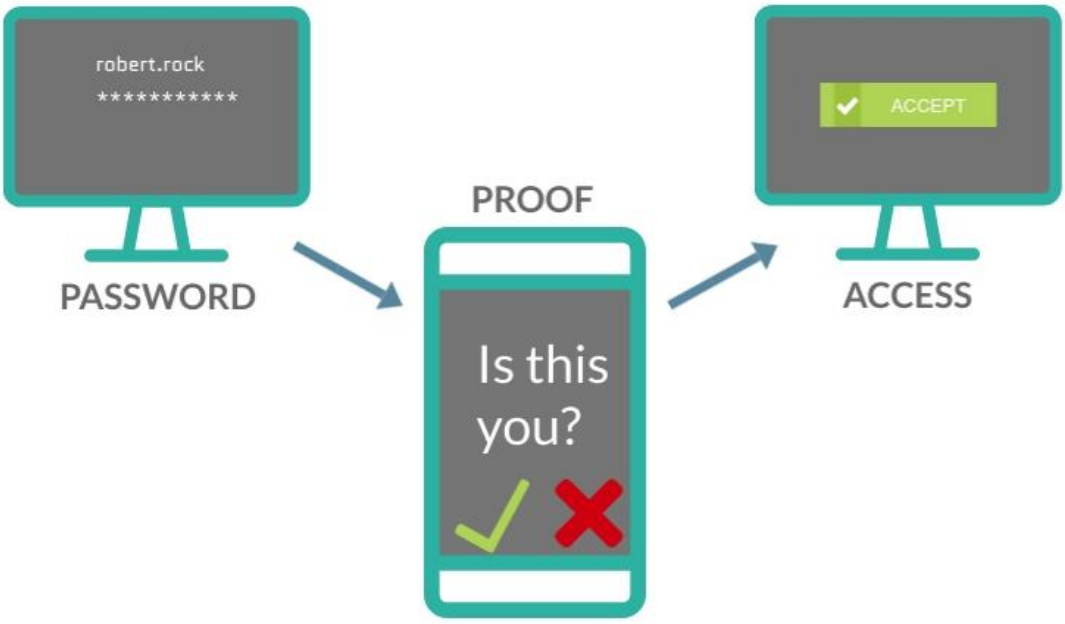

Figure 4. Multi-factor Authentication example

Following common safety practices, most day-to-day user threats can be eliminated quite effectively. Employees of an organization that handle any sensitive information should be further trained and brought up to the possible security vulnerabilities their actions could cause. Statistics from a research report commissioned by Egress (2019) show that 60% of the data breaches during 2019 were caused by human error. Large part of information security management systems (ISMS) like the ISO/IEC 27001 standard, focus on combating human error.

2.3 Information security management system (ISMS)

An information security management system is a collection of procedures and policies that addresses all aspects of creating and maintaining a secure information environment in an organization. ISMS provides consistent and systematic approach to processes, technology and people through effective risk

management (URM Consulting 2020). ISMS systems vary on their methods used and how they are constructed. There are some heavily tailored solution packages for certain types of organizations. Private vendors usually provide more restricted information security management systems when it comes to the controls used.

2.3.1 ISO/IEC 27001 standard

The ISO/IEC 27000 family is a collection of information security standards published by International Organization for Standardization, with a purpose of detailing how to create, implement and manage controls and policies. With the world-widely recognized effectivity of the standard comes trust. Companies implementing the standard can get credited certifications upon passing an audit. In technology-driven industries, these give organizations market capitalization (ISO Committee 2018).

ISO/IEC 27001 is the most used standard of the family with over 40,000 certificates in 2017 and estimated annual growth of 20% (ISO Commitee 2018). The purpose of the 27001 standard is to preserve the three principles of information security, the CIA Triad. The security of the 27001 bases on policies, security processes and activities working to complement of each other (Figure 5).

Figure 5. ISO/IEC 27001

The controls used are not assigned to the standard. Instead the companies are free to choose most fitting options from an assortment of controls noted in the list

of controls called Annex A (ISO Commitee 2018). An organization must do their own risk assessment, in order to plan a successful ISMS. Disterer (2013) published an article where he described the main key points of ISO/IEC 27001 controls to be:

- Operating procedures
- Passwords and use of password management systems
- Encryption of confidential information
- Legal obligations
- Employee awareness and training

The assessment of organizations need for standardized security measures determines if implementing an ISMS is in order. Implementing the 27001 standard can be reasonable if the organization strives to indicate the level of information management for its customers as well as their own data. Or, if the organization finds it justifiable to make sure security that vulnerabilities are found and eliminated or minimized from their own systems (ISO Commitee 2018).

3 HACKING

Hacking is a wide term used for activity where a person gains access to a system or a network in an unauthorized manner. That access can then be used to control systems, steal data or disrupt activity. (Technopedia 2020.) In 2018, there were 18.4 billion network connected devices and the number is estimated to reach 29.3 billion by 2023 (Cisco 2020). Every single one of these devices is vulnerable to hackers. Hacking is a massive concern in the information technology world, and it is becoming more and more prevalent due to our reliance of technology.

3.1 Motives

The objective of a hack may be malicious or benevolent. Whether the hacker uses his access to harmful purposes or not, can be used to categorize him. Most commonly hackers are divided into three groups based on the information by Zetter (2016). The three categories of hackers are as follows:

Black hats practice illegal hacking, the criminals hacking for personal gain. They attack a system or network using software holes or zero-day attacks with malicious intent, such as stealing information or destroying files. They may also sell information about vulnerabilities for other black hat hackers to use. The result of the black hats' actions is that someone always suffers from it, whether it's the organization or the general public.

Grey hats, act without permission of the target, but without malicious intent. They may sell or disclose zero-day vulnerabilities to someone with expected good intentions. Grey hats could break into secure systems of an organization without authorization to do so. After they would report of the vulnerabilities he discovered, possibly requesting financial compensation of the information given. Grey hats may offer their services to fix the found vulnerabilities as well.

White hats try to discover vulnerabilities with permission of the target in the system and then notify of them, so that they can be fixed. White hats are usually the paid employees, advisors and specialists that work for or with the organizations. White hats that are not associated with any organization can still use their skills for the good with bug bounty programs. Companies offer programs where the hacker can sell his information about a vulnerability for a reward.

The various sides of hacking tends to paint a picture of good and bad hacking. Although the world of hacking is not as clear cut as demarcating goodness and badness with bold lines and hat colors. The motives and repercussion of their actions can differ. Black hats could be causing massive financial damage or disrupting critical services, or just snooping around in unauthorized systems, because they can. Sometimes hackers' actions can be seen to be with good or bad intentions depending on the audience. For example, a hacker could leak confidential information concerning unethical actions to the public. (Knowles 2016.)

In the eyes of general public, term hacking associated mostly with negativity, crime and havoc. This is mainly because media paints a picture of all hackers

being these mysterious criminal geniuses. Very often, people who hack are just enthusiasts who love to manipulate things to work outside their intended way. A very small portion of these people will ever end up doing anything remotely prohibited. Ethical hackers such as penetration testers more than likely started doing these things as a hobby and later found a career in them. Hacking is just like a tool. What we choose to do with it is up to us. (Knowles 2016.)

3.2 Methods

The description of attack types in this section bases on the article by Kumar (2018). Not all hacks are technical, software-based attacks, in fact, the biggest vulnerability in computer information security is the end users. Attackers will use the largest vulnerability available to breach systems. Understanding

Social engineering is an act of using social behavior to manipulate people to gain access to restricted areas. Impersonating is the most common way of achieving this, falsely posing with authority or gaining victims' trust to get confidential information. Phishing is a practice of using emails, phone calls or text messages. Contacts appear to come from reputable sources in order to obtain personal information or influence their actions. Other means of nontechnical attacks can include physical copies of protected information being mishandled and ending up in wrong hands.

Network foundation attacks can come from anywhere in the world to the target through the internet. Attacks using network vulnerabilities often use existing traffic, or in some cases waste traffic, to carry out the attacks. Examples of network-based attack types could include exploiting transport protocol weaknesses from protocols such as TCP/IP or PPTP is often used, if they are not properly set up. Waste traffic can be used as denial of service (DoS), done by flooding the computer with excess number of packets to disrupt network activity or completely bring down operations. Man-in-the middle attacks (MITM) happen when the attacker secretly listens to or modifies the traffic between two parties

(Figure 6). For example, packet sniffing, a form of eavesdropping, is a method of capturing packets from a network and reading its contents.

Figure 6. Man-in-the-middle attack

Operating systems are the most common target for finding vulnerabilities, since every device is running one. Computers run operating system specific protocols, and these get often exploited. Machines running on the old versions of the operating systems are more prone to vulnerabilities. Some of the more niche operating systems can be more secure options. For example, OpenBSD is considered the most secure general-purpose OS available (Palmer & Nazario 2005). Mostly, hackers focus on targeting the broadly utilized operating systems like Windows, because their vulnerabilities are better known.

Application attacks are the most widespread type as the methods usually involve email servers and web applications. Common protocols such as Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) have usually full access over firewalls, which is why the applications with these protocols are often targeted. Malicious software (malware) infects a system with various intents. Common malware types are, worms, trojans and spyware. A worm replicates itself spreading over a computer network. Trojans distinguish themselves as legitimate software to fool the user to allow access. And spyware collects information without the user’s knowledge, via keylogging for example.

Ransomware is another type of malware that has seen rapid growth in use over the past 10 years. Ransomware works by holding data for ransom, by encrypting the data, for example. The new trend of ransomware attacks appeared when cryptocurrencies became more widely available (Fruhlinger 2020). Spam mail has been witnessed by every internet user and is still very prevalent, as it is still the most efficient way for cybercriminals to spread infectious software throughout the internet and it has impacted email storage framework. Email addresses are collected from various websites that don't protect this information and then these addresses are targeted with spam mail. Spam mail contributed to 45.3% of total email traffic in 2018. (Clement 2019.)

4 DATA BREACHES

Data breach stands for a loss of private or confidential information to an unsecure audience. Data breach can result from an accident just as well as a deliberate attack. Any organization could become a victim of a data breach, but the information that gets leaked determines the outcome and effects it will have. Strawbridge (2020.)

4.1 Effects of data breach

Strawbridge (2020) wrote a publication on Metacompliance where effects of data breaches were discussed. Data breaches affect millions of people around the world and it's on the rise. Many companies have suffered from a data breach, leading to layoffs, lawsuits and fraud. Once these criminals have our information, they can use it to their personal gain in multiple ways. Most notably, criminals will try to get financial gain from their attacks in form of stealing. Data breach also often results in identity theft, allowing someone else to use your name for their gain. In some cases if the victim has information that they don't want to be made public and the cybercriminal gets hold of it, they might use that for blackmail. Although the objective of the attack may not always be direct financial gain, the effect of a data breach almost always ends up costing the organization financially.

Risk based security research report (2019) states that in 2019, the reported number of breaches was 7,098. With these breaches, more than 15.1 billion compromised records were exposed, which is a 284% increase from the total number of records exposed in 2018.

As the number of data breaches rises, and the exposed record count finds new heights, should organizations also work towards improving their security. Unfortunately, the correlation is not there yet. Strawbridge (2020.)

Financial loss

Number of attacks each year is growing constantly and the financial effects it has on the organizations is also growing. Based on the study found in Cisco Annual Cybersecurity Report (2018), 53% of all attacks had a financial damage of USD$500,000 or more (Figure 7). This number includes lost revenue, customers, opportunities and out-of-pocket costs.

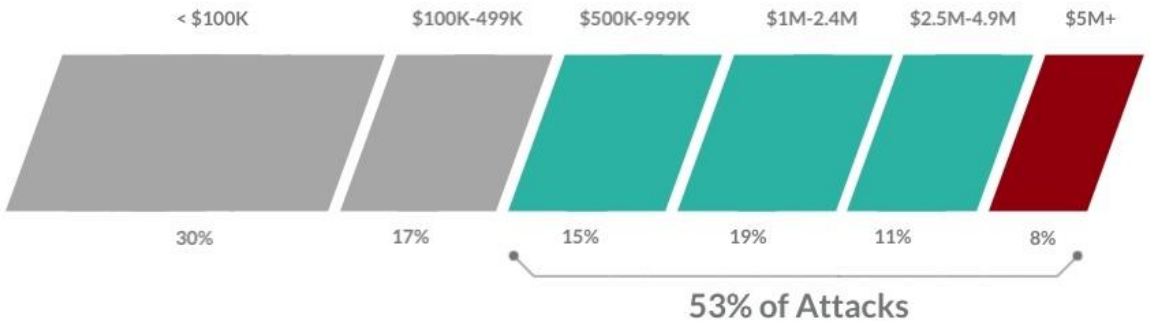

Figure 7. According to Cisco's annual cybersecurity report, cost of damages caused by attacks exceeding USD$500,000 fifty-three percent of time.

Direct financial damages are just the first step of paying up for the lapse in security. More than likely, organizations will feel the financial loss of a data breach well into the future. When the world knows about the incident, people will start doubting their trust on the organizations, causing reputational damage.

Reputational damage

In today's age of hyper-connected world, news could reach the entire world in matter of seconds through social media. This means that any defamatory news

towards a company could lead into devastating reputational damages. And we know the internet is a ruthless place when it comes to criticism. A survey research by Ponemon Institute (2017, 12) indicates that 65% of people affected by a data breach lost trust in the organization, while 27% discontinued relationship with organization. This is why it is important to handle the aftermath of a data breach properly; it requires taking responsibility of the actions that caused the vulnerability. Financial losses caused by the reputation of the organization being damaged are impossible to calculate. The stigma will hold for a long time and lead to missed business opportunities.

Operational disruptions

Galvin wrote an article for Inc (2018) describing the result of a cyberattack. When a small and midsize businesses are attacked, it results in the companies having to go into recovery mode. Seizing all operations to find the cause and solution to fix it can cause smaller businesses to fall completely out of the map. According to the report referred in the article, small and midsize business can’t handle the downtime in operations, causing 60% of them to be out business within 6 months.

Business being down for a prolonged period of time affects the reputation and obviously the financial status of the organization as well. Larger organizations may survive and recover from operational disruptions, but they will definitely feel the effects. The Affected number of people is usually somewhat relative to the size of the organization. More downtime means more people affected.

Legal ramifications

The following bases on the page on Iron Mountain (2020) where the legal ramifications of a breach are discussed. Any time an organization ends up in court as a result of a data breach, it will most definitely end up costing the organization largely. Consequences can include government fines, penalties, and in some cases, even jail time may be sentenced. For large data breaches, the settlements can reach over USD$100 million.

4.2 Major incidents

In the past years, many of the names associated with trust and security, have been victims of a data breach. Large organizations with empire like infrastructures and seemingly endless budgets still get breached. Looking into 3 major incidents we have had to get an idea of how these massive breaches happen and what results from them.

Facebook

Isaac (2018) wrote an article on New York Times, going over how Facebook data breach occurred, exposing personal information of nearly 50 million users. The breach occurred in March of 2018 where attackers were able to use Facebook's features implemented to improve privacy against themselves. A feature "View As" that allows users to see what information others can see from your profile had a glitch where it could be used to see users contacts without being on their friend list. Another tool on the website that contained flaws was a video uploading tool introduced to allow easy upload for birthday videos. The bugs from these features along with other software flaws in Facebook's systems allowed attackers to access user accounts. Facebook has later reported that the issues have been fixed and have started investigation. Facebook has also been on the news regarding account information being harvested for political use.

Yahoo

In 2016, Yahoo!, a web service provider, disclosed that it had suffered two data breaches, one in 2013 and another in 2014. The affected number of accounts reaching 3 billion accounts. (Al-Heeti, A. 2018.) A Blog by Williams (2017) on CSO explained how the attack was done. Investigations by the Federal Bureau of Investigations (FBI) show that the attack started from a spear-phishing email sent to the employees of Yahoo. Spear-phishing emails are targeted emails containing malicious software behind a link or a button embedded into the email. If one person mistakenly then clicked on the said link, the malware would infect the computer. This allowed the attacker to access and control Yahoo's user database. The attacker was able to steal a copy of the database. The database

targeted contained names, phone numbers, password recovery emails and cryptographic value called nonce, assigned uniquely to every account.

In December 2016, Yahoo came out with the full report with details and recommended all users to change their passwords. During this time, Verizon Communications and Yahoo were in negotiations of an acquisition deal for USD$4.8 billion. Because of the data breach, the price was later discounted by USD$350 million. (Kirk. 2017.)

Equifax 2017

American multinational consumer credit reporting agency, Equifax, is the victim of a large data breach. Based on the settlement found in Federal Trade Commission (FTC) (2020), the personal information of 147 million people was exposed in September 2017. Equifax agreed to a global settlement with the FTC to help people affected by the data breach. This could cost the company up to USD$425 million. If person was a victim of identity theft or fraud related to the breach, they could file a claim to cover expenses.

The report by GAO (2018) regarding the incident explains how the attack took place and what the impact of it was. In March 2017, unidentified attackers found a vulnerability via consumer complaint web portal. Using the known vulnerability in software Equifax was running on the portal, attackers gained access to the system. Using A number of techniques to disguise their actions on the systems and on the database queries their applied, attackers were able to retrieve personal information from the databases (Figure 8). Leveraging existing encrypted communication channels, the attackers were able to blend in and send requests while remaining hidden on the network.

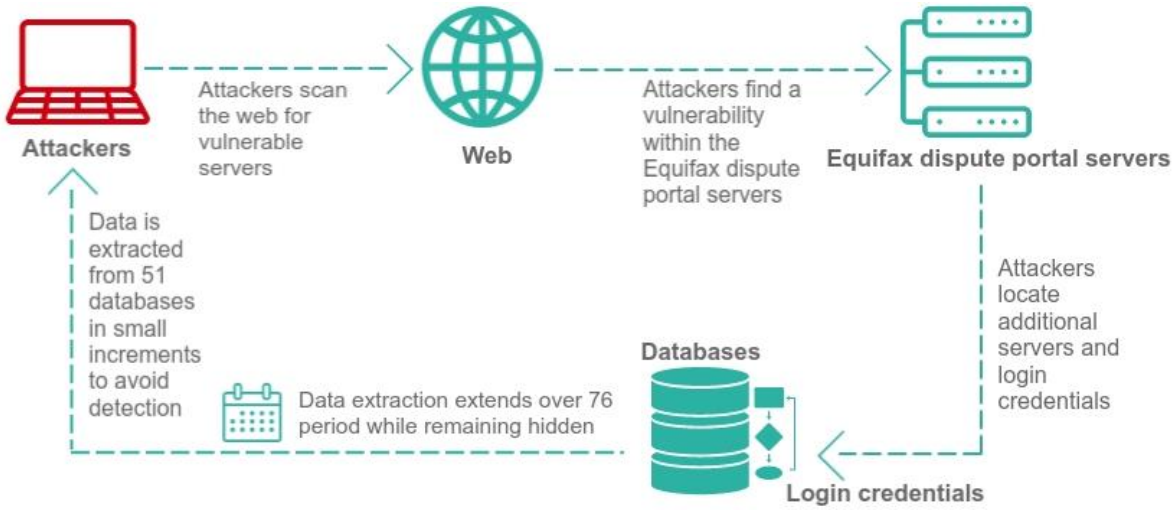

Figure 8. Equifax data breach structure explained in the report by GAO

In July 29, Equifax discovered the breach and took actions to address the vulnerabilities that allowed the attackers to successfully breach their systems. The company issued a report concerning the breach to notify users that it had taken steps to identify, notify, and provide support to those affected by the breach. (GAO 2018.)

5 PENETRATION TESTING

As the practical part of the thesis, I examine and perform a packet sniffing hack and scan a web server for vulnerabilities on a virtual environment, while learning about penetration testing environments used in ethical hacking and as a research platform. These example hacks are a small-scale simulation to show as proof-of-concept on how hacking can take place. The purpose of the hack is to show how easy it could be to retrieve data over an unsecure network where the privacy of the connected devices is compromised or attack a website that doesn't have the required safety standards set in place.

I will run the virtual environment on my own personal computer. Virtual machines will be connected to a virtual network adapter to create a secluded network in order to avoid the vulnerabilities introduced to the virtual environment from reaching the real network.

5.1 Tools

For the hypervisor, I chose to use Oracle VM VirtualBox. An open source virtual machine platform. For my task, I require the virtual machines that act as the victim and the attacker. Kali Linux is the platform I will use for my attacker machine. Kali is a Debian based distribution by Offensive Security which is designed for penetration testing and research. Kali Linux comes pre-installed with many of the tools required in penetration testing, such as wireshark. Offensive security also provides a virtual machine image called metasploitable that acts as a victim. Rapid7 (no date) has an metasploitable introduction and setup guide page, that describes the machines capabilities and purpose. Metasploitable 2 is of a virtual machine designed as intentionally vulnerable to use for training, testing and to practice common penetration techniques. Vulnerabilities included in the metasploitable machine include many of the common vulnerabilities found for example, on web applications. It is important to never introduce metasploitable image to your real network. I also need a victim machine that will communicate with the metasploitable machine, and for that I chose to use Windows 10.

The list of all the software installed includes the following

- Oracle VM VirtualBox 6.0.20
- Kali Linux 64-bit 2020.1
- Metasploitable 2 64-bit
- Windows 10 64-bit 1909

With this environment, we can train and practice on the most of the vulnerabilities metasploitable 2 offers. With metasploitable, required skill level of hacking varies from entry-level to challenging even the most enthusiastic cyber security experts.

5.2 Penetration testing lab setup

In order to create the safe environment that allows for the test to take place a couple of key points must be set properly.

We need to create and configure the Virtual Host-Only Ethernet Adapter to our VirtualBox (Figure 9). Adding network adapters to VirtualBox 6.0.20 happens from network settings tab, which can be found from:

Tools > Network > Create

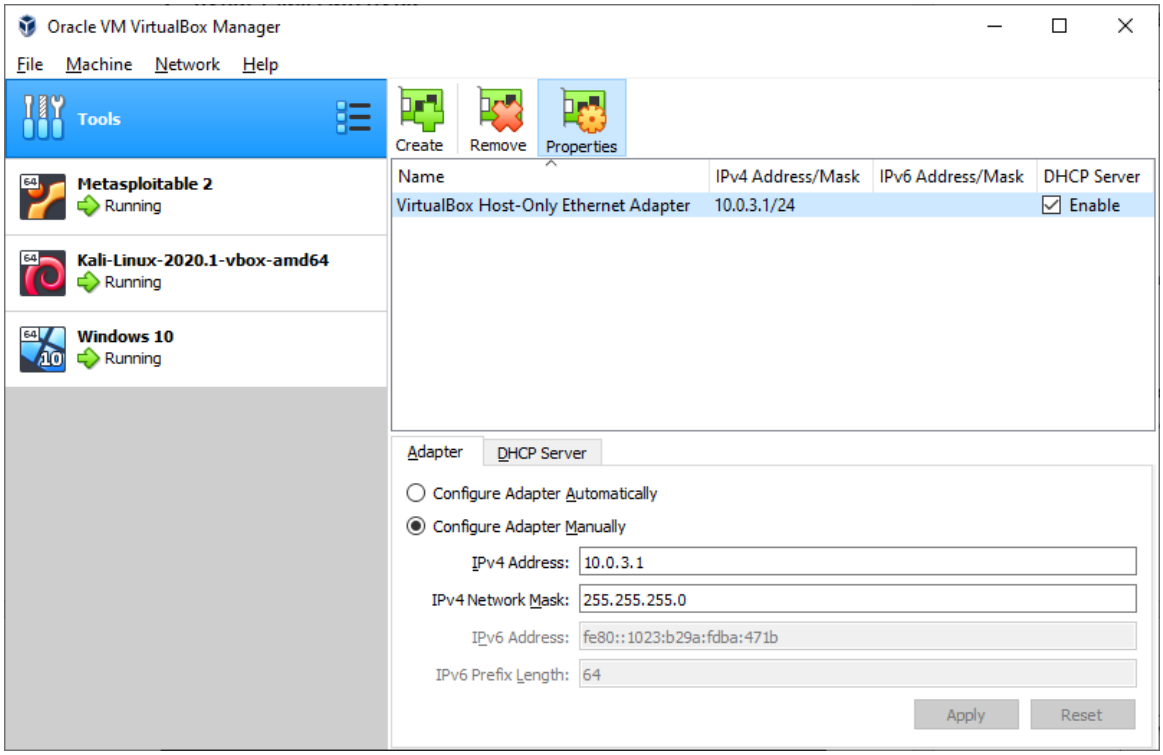

Figure 9. Virtual Host-Only Ethernet Adapter

With the virtual adapter enabled, each virtual machine needs to be set to use the Host-Only adapter on promiscuous mode. Promiscuous mode allows the adapter to read network packets in their entirety. Every virtual machine needs to use only this adapter and have no other adapters enabled. Attaching the virtual machines to the Host-Only Adapter and setting the promiscuous mode can be done by navigating to the following:

Select virtual machine > Settings > Network

With the metasploitable 2 machine running, we determine the IP address of the machine by running *ifconfig* on the shell as follows:

IP-address of metasploitable machine: 192.168.56.101

To test if we have a connection between machines and can access the metasploitable page we can use web browser on one of the machines, enter the IP-address of the metasploitable to the address bar. If working correctly we should be greeted with the metasploitable front page (Figure 10). On our test, we will use the mutillidae web page.

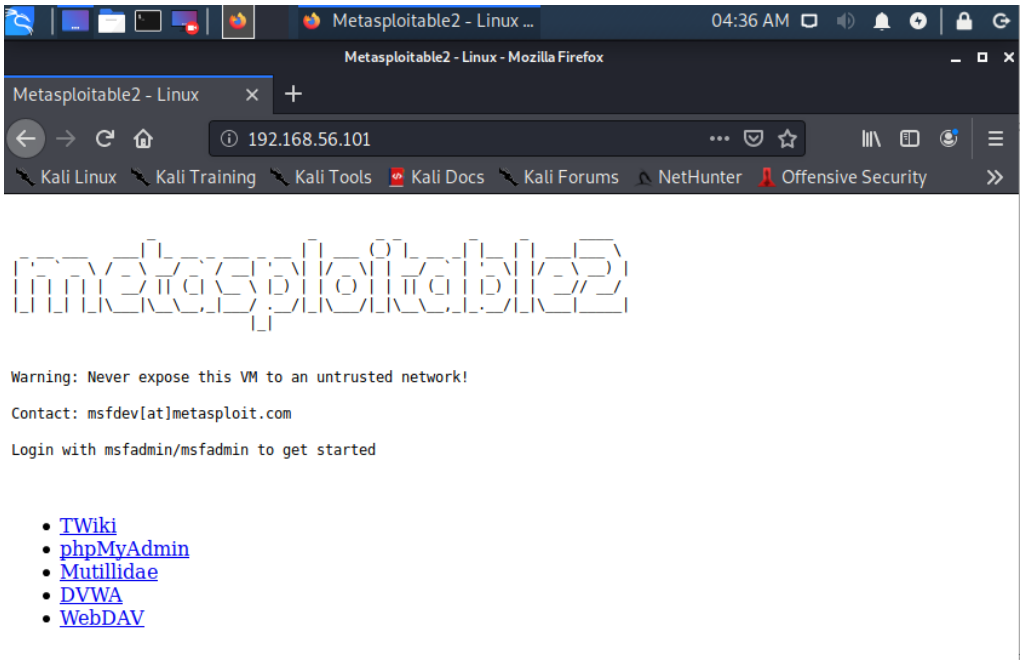

Figure 10. Accessing the metasploitable front page from another system

5.3 Packet sniffing hack

In this simulation, a computer is trying to communicate with a web page over an untrusted network. This could just as happen over a free Wi-Fi in a café shop, for example. The victim using the untrusted network is communicating with a web page that is running Hypertext Transfer Protocol (HTTP) instead of Hypertext Transfer Protocol Secure (HTTPS). Web browsers will usually have a tab before the address that inform whether the connection is safe or not (Figure 11). Or, it will have *http:// or https://* in the beginning of the address.

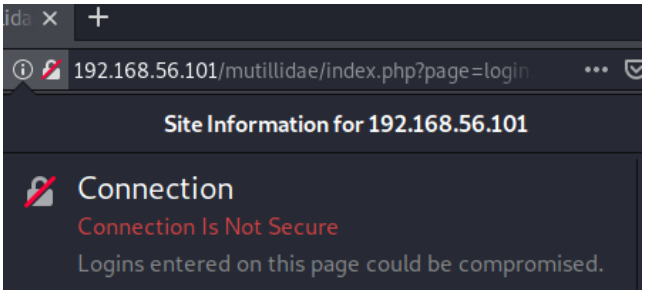

Figure 11. Firefox notification of an unsafe connection

To perform the simulation, the Windows 10 victim machine will use the login page found on the mutillidae web page. The attacker connected to the same untrusted network is capturing traffic and gets the packet containing the victim's login credentials (Figure 12). Because the traffic is not encrypted, the packets may contain sensitive information in legible form.

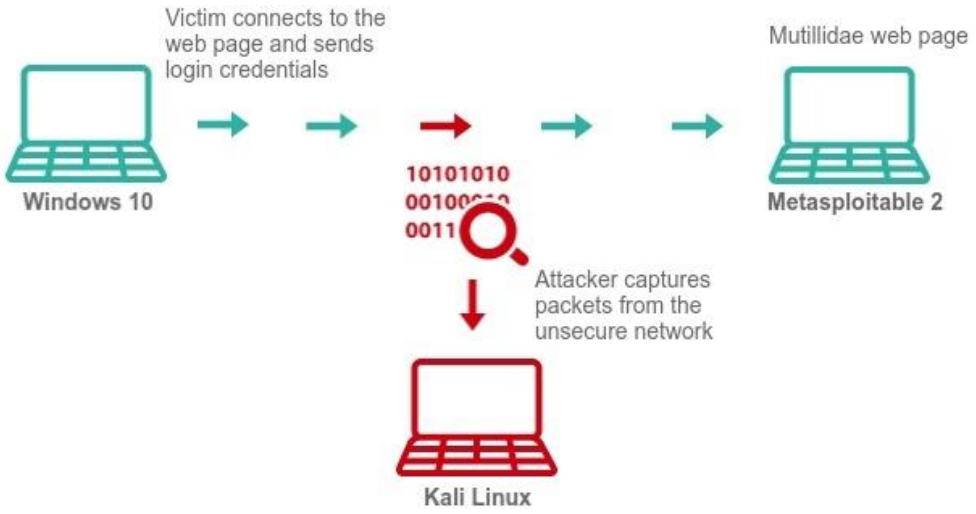

Figure 12. Packet sniffing hack

Kali Linux comes preinstalled with multiple sniffing tools. I chose to use the network analyzer, Wireshark. All I need to do with Wireshark is to select the interface I want to capture from, in this case the host-only network adapter and select *Start capturing packets.* From Windows 10 machine, navigating to the *login/register* page of mutillidae, we can enter our login credentials (Figure 13).

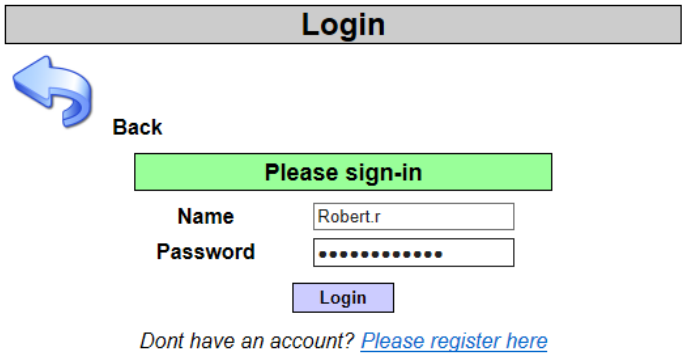

Figure 13. Victim's login credentials

When the *Login* button is pressed, the packet is on its way over the network to the web page. After the attacker has captured the traffic, he can start going over the packets to see if anything that indicates to website user traffic.

5.3.1 Packet analysis

With the captured traffic, packets that won't include anything that concerns us need to be filtered out, using key string to look for packets that may include the right packets. Packets sent to HTTP will often use the POST method. Using POST as a key string to filter out packets, we can search for vulnerable packets. This is shown in Figure 14.

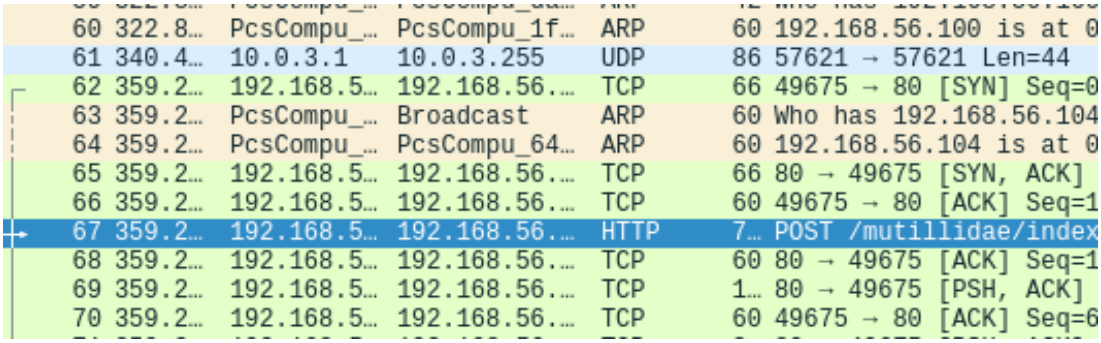

Figure 14. Captured traffic containing vulnerable packet

Analyzing the packet, it becomes apparent that no encryption was applied on the packet, before it reached the attacker's machine. Login credentials are found under the HTML Form, in clear legible form (Figure 15).

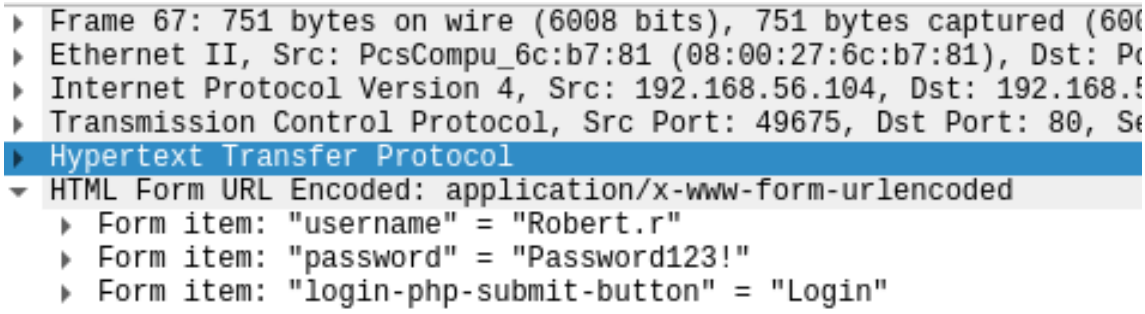

Figure 15. Compromised packet contents

In the worst-case scenario, it could that easy to steal your personal information with packet sniffing. When communicating with a web page, it's important to always check if the site is running HTTPS.

5.4 Scanning a web server

Finding possible vulnerabilities from a web server can be achieved via web server scanners such as Nikto, which comes preinstalled on Kali Linux. According to Kali Tools (2014), Nikto runs comprehensive tests on the web server for possible vulnerabilities, that include 6 700 potentially dangerous files or programs. Nikto will also recognize outdated or version specific flaws of thousands of servers. To learn how to structure the nikto command line, we can input a command showing all the possible nikto options as follows.

kali@kali:~$ nikto -H

Using mutillidae as our example web page again. We can run a test scan on the metasploitable web server from the Kali machine by composing the following command line on the terminal. This will create a report file in html format on our current directory.

kali@kali:~$ nikto -host 192.168.56.101 -root /mutillidae
$(pwd)/mutillidae.nikto.html -Format HTM

To inspect the generated report, we can use a web browser, in this case Firefox. Opening the file with Firefox can be done with a simple following command line.

kali@kali:~$ firefox mutillidae.nikto.html

The report includes vulnerable and improperly set technologies used in the web server and explains where the vulnerability is (Figure 16).

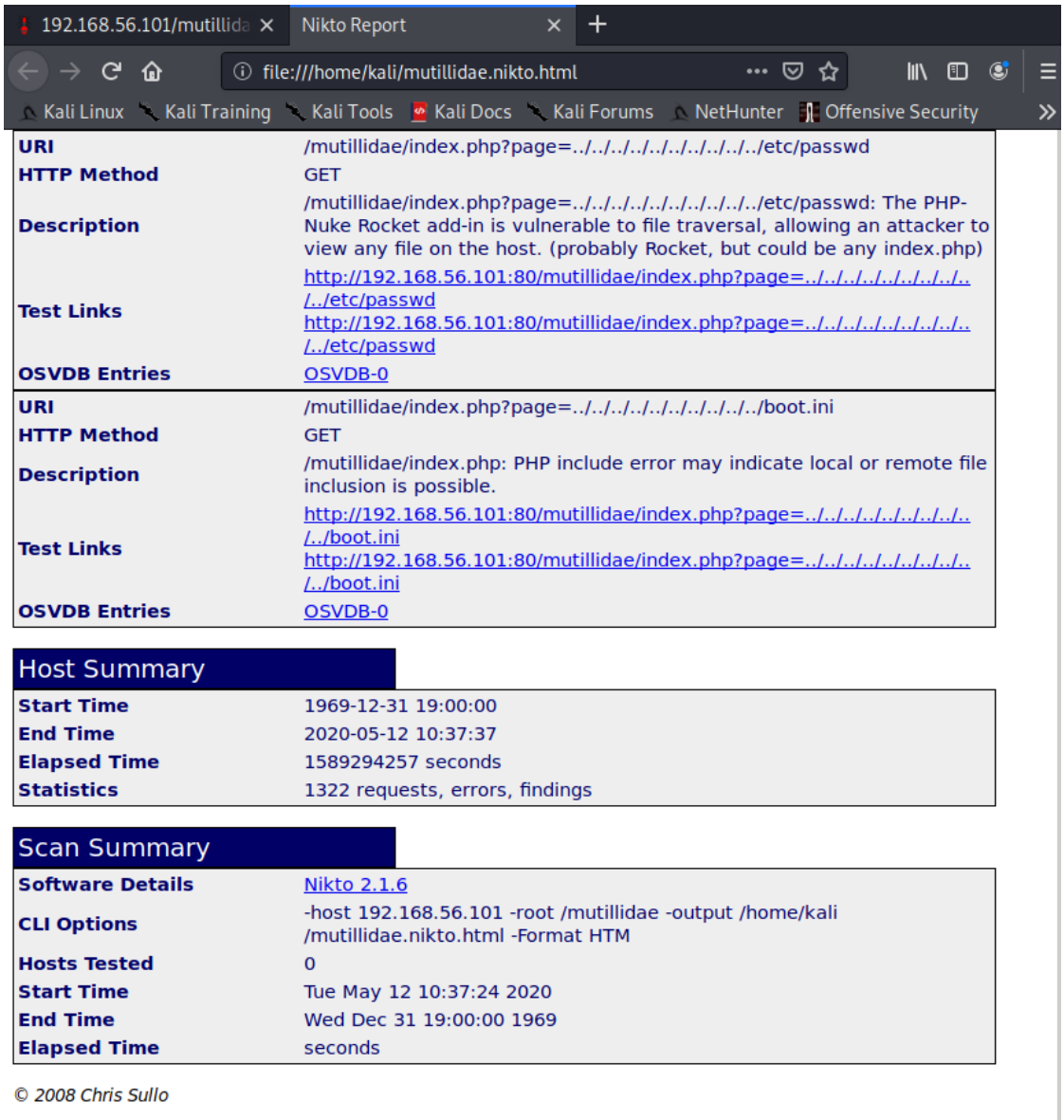

Figure 16. Nikto scan report

As Figure 16 shows, Mutillidae scan included 1 322 requests, errors and findings. Since mutillidae is flooded with intentional vulnerabilities, the scan result was massive. In real-life situation, it could only require one flaw to result in a breach. Scan like this was used to find the vulnerability that started the Equifax data breach.

6 CONCLUSIONS

With the purpose of learning about organizational information security through research, statistics and observations, my thesis work was enlightening. Along the process of the work, I got a broad overview into how serious and ever growing issue cybersecurity is to every organization. The potential effects a data breach can have even on an established organization is astounding. Tackling the issue of security means considering much more than just the technological factors. As it stands, human error is the number one cause of lapse in security. No fancy technology protocols can fix mistakes made by a human. Organizations need to focus more on end-user security awareness training in order to combat the vulnerabilities caused by human error. Hackers are not only roaming the internet, although their presence in the real world can be hard to detect. Methods used by hackers vary from social engineering to the most technical and overwhelmingly complicated executions.

When I studied the penetration testing environments, I got really interested in penetration testing and will pursue it further beyond after this thesis. All the sample work I did on this thesis were a proof-of-concept for the theory part. The introduction and exploration of different vulnerabilities and methods helped me piece together an understanding of how real-life situations come up. The best way to prevent attacks is to understand how they are constructed in the first place.

Considering the findings from this thesis work, although cybersecurity has come a long way in the past ten years, a lot is left to be desired from organizations. More awareness, training and standardization of policies and controls will be the direction many will need to start heading to, if they want to continue secure operations.

REFERENCES

Al-Heeti, A. 2018. WWW document Yahoo must pay $50M in damages for security breach. Available at: https://www.cnet.com/news/yahoo-must-pay-50m-in-damages-for-security-breach/ [Accessed 9 May 2020].

Artur Victoria. 2019. Information Security. PDF document. Available at: https://www.researchgate.net/publication/331833287_Information_Security [Accessed 14 April 2020].

Cisco. 2020. Annual Internet Report (2018-2023) Whiter Paper. WWW document. Available at: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html [Accessed 9 April 2020].

Cisco. 2018. Annual Cybersecurity Report. PDF document. Available at: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf [Accessed 1 May 2020].

Clement, J. Spam: share of global email traffic 2007-2018. WWW document. Available at: https://www.statista.com/statistics/420400/spam-email-traffic-share-annual/ [Accessed 13 April 2020].

Cloudfare. What is Encryption? WWW document. Available at: https://www.cloudflare.com/learning/ssl/what-is-encryption/ [Accessed 10 May 2020].

CSO. 2020. Recent ransomware attacks define the malware's new age. Blog. Available at: https://www.csoonline.com/article/3212260/recent-ransomware-attacks-define-the-malwares-new-age.html [Accessed 7 May 2020].

Fahey,R. 2019. Security Awareness For End Users WWW document. https://resources.infosecinstitute.com/category/enterprise/securityawareness/security-awareness-roles/security-awareness-for-end-users/ [Accessed 8 May 2020].

Federal Trade Commission. 2020. Equifax Data Breach Settlement. Available at: https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement [Accessed 10 May].

Fruhlinger, J. 2020. Blog. Available at: https://www.csoonline.com/article/3212260/recent-ransomware-attacks-define-the-malwares-new-age.html [Accessed 13 April 2020].

Galvin, J. 2018. 60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack. WWW document. Available at: https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html [Accessed 10 May].

GAO. 2018. Actions Taken by Equifax and Federal Agencies in Response

to the 2017 Breach. PDF document. Available at: https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf [Accessed 9 May 2020].

Georg Disterer. 2013. ISO/IEC 27000, 27001 and 27002 for Information Security Management. PDF document. Available at: https://serwiss.bib.hs-hannover.de/frontdoor/deliver/index/docId/938/file/ISOIEC_27000_27001_and_27002_for_Information_Security_Management.pdf [Accessed 15 April 2020].

Isaac, M. 2018. Facebook Security Breach Exposes Accounts of 50 Million Users. Blog. Available at: https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html [Accessed 10 May].

Infosec. 2015. End User Security Awareness Best Practices: 12 Experts Weigh In. Available at: https://resources.infosecinstitute.com/end-user-security-awareness-best-practices-12-experts-weigh-in/ [Accessed 10 May].

Iron Mountain. 2020. WWW document. Available at: https://www.ironmountain.com/resources/general-articles/t/the-legal-ramifications-of-a-data-breach [Accessed 9 May 2020].

ISO Committee. 2018. ISO Survey of certifications to management system standards. WWW document Available at: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1 [Accessed 15 April 2020].

Jouini, M., Rabai,L.B.A., Aissa, A. B. 2014. PDF document. Available at: https://core.ac.uk/download/pdf/82369839.pdf [Accessed 13 April 2020].

Kali Tools. 2014. Nikto Package Description. Available at: https://tools.kali.org/information-gathering/nikto [Accessed 10 May 2020].

Keung, H.Y. 2014. Basic Principle of Information Security. PDF document. Available at: https://www.hilarispublisher.com/open-access/basic-principle-of-information-security-2168-9695.1000e120.pdf [Accessed 14 April 2020].

Kim Zetter. 2016. Hacker Lexicon: What Are White Hat, Gray Hat, and Black Hat Hackers?. WWW document. Available at https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/ [Accessed 9 April 2020].

Kirk, J. 2017. Yahoo Takes $350 Million Hit in Verizon Deal. Blog. Available at: https://www.bankinfosecurity.com/yahoo-takes-350-million-hit-in-verizon-deal-a-9736 [Accessed 10 May].

Knowles, A. 2016. How Black Hats and White Hats Collaborate to Be Successful. WWW document. Available at: https://securityintelligence.com/how-black-hats-and-white-hats-collaborate-to-be-successful/. [Accessed 10 May].

Onelogin. 2019. How does Multi-Factor Authentication work? Available at: https://www.onelogin.com/learn/what-is-mfa [Accessed 10 May].

Option matters. 2019. Insider Data Breach survey 2019. PDF document. Available at: https://scoop-cms.s3.amazonaws.com/566e8c75ca2f3a5d5d8b45ae/documents/egress-opinionmatters-insider-threat-research-report-a4-uk-digital.pdf [Accessed 10 May].

Palmer, B., Nazario, J. 2005. Overview of OpenBSD. WWW document. Available at: https://www.informit.com/articles/article.aspx?p=363732&seqNum=2 [Accessed 13 April 2020].

Pixelprivacy. 2020. Password managers. WWW document. Available at: https://pixelprivacy.com/password-managers/ [Accessed 5 May 2020].

Ponemon Instutute. 2017. PDF document. Available at: https://www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf [Accessed 9 May 2020].

Rapid7. 2020. Metasploitable 2 Exploitability Guide. Available at: https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide [Accessed 1 May 2020].

Risk Based Security. 2020. Number of Records Exposed in 2019 Hits 15.1 Billion. WWW document. Available at: https://www.riskbasedsecurity.com/2020/02/10/number-of-records-exposed-in-2019-hits-15-1-billion/ [Accessed 8 May 2020].

RSI Security. 2019. What Is The Purpose of Information Security Access Controls? Blog. Available at: https://blog.rsisecurity.com/what-is-the-purpose-of-information-security-access-controls/ [Accessed 15 April 2020].

Sunil Kumar. 2018. Hacking Attacks, Methods, Techniques And Their Protection Measures. PDF document. Available at: https://www.researchgate.net/publication/324860675_Hacking_Attacks_Methods_Techniques_And_Their_Protection_Measures [Accessed 9 April 2020].

Technopedia. 2020. Hacking. WWW document. Available at: https://www.techopedia.com/definition/26361/hacking [Accessed 9 April 2020].

URM Consulting. 2020. What is an ISMS? Why should you implement one? Blog. Available at: https://www.urmconsulting.com/2020/02/18/what-is-an-isms-why-should-you-implement-one/ [Accessed 15 April 2020].

Williams, M. 2017. Blog. Available at: https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html [Accessed 9 May 2020].